REMARKS/ARGUMENTS

The Examiner rejected claims 1, 3, 4, 7-12, 14-16, 18-27, 29, 30, and 33-40 as anticipated (35 U.S.C. §102) by Ross (U.S. Patent No. 5,182,77). Applicants traverse for the following reasons.

Independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined code if there is one determined code; processing the decrypted response to determine whether the second computer system is authorized to access the software; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

The Examiner cited col. 7, line 23 to col. 8, line 24 of Ross as disclosing the requirements of these claims. (Final Office Action, pg. 2) Applicants traverse.

The cited cols. 7-8 describe an enablement process that runs on the system in which the licensed software is installed. The enablement process prompts an installer to select a product type, version or product name, serial number, etc, which the installer communicates to a fulfillment agent. The fulfilment agent accesses an enabler key database based on the product type, serial number and extracts the appropriate enabler key, which the fulfillment agent communicates to the installer. The installer provides the enablement key to the enabling process, which checks if the key is correct. If the enablement key is correct, the license is enabled. The enablement key decrypts the encrypted part of the license and is made available to the installer upon payment of the purchase price.

Nowhere do the cited cols. 7-8 anywhere disclose the claim requirements that the first computer system, the one providing the software, receive a request for software from the second computer system, on which the software is to be installed, then transmits an encrypted message to the second computer system, and then receives an encrypted response from the second computer system. Instead, the cited cols. 7-8 discuss how an installer on the computer to receive

the software sends information to a fulfillment agent, and then receives an enabler key which the enabling process uses to activate the license. Nowhere do the cited cols. 7-8 anywhere disclose that the computer to receive the software send a message and then the computer providing access to the software send an encrypted message, and then also receive a response to such encrypted message. Instead, in the cited Ross, the computer that receives the software only sends one message to obtain the enablement key, not the claim requirements of first a a request then a message in response to an encrypted message as claimed.

Further, nowhere do cited cols. 7-8 anywhere disclose the claim requirements that the computer that grants access to the software, which in the cited Ross appears to be the fulfillment agent, performs the claim requirements of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined code if there is one determined code. Instead, the cited cols. 7-8 discuss how the installer transmits to the fulfillment agent the product name, serial number and number of connections, and the fulfillment agent uses this information to access an enabler key from the key database to return to the installer. Nowhere does the cited Ross anywhere disclose that the fulfillment agent determines whether a code has been made available by the computer on which the software is to be installed that is capable of decrypting the received encrypted response and decrypting the encrypted response with the determined code if there is one determined code. Instead, in the cited Ross, the fulfillment agent accesses an enabler key from the enabler key database based on product type, serial number, and the number of connections information transmitted by the installer.

Moreover, nowhere does this cited Ross disclose the claim requirement of determining whether the computer or system on which the software is installed has made a code available that is capable of decrypting a received encrypted response from the user as claimed.

Accordingly, claims 1, 16, and 27 are patentable over the cited art because the cited art does not disclose all the requirements of these claims.

Claims 3-4, 7-11, 14-15, 18-26, 29, 30, 33-40 are patentable over the cited art because they depend, directly or indirectly, from one of claims 1, 16, and 27. Moreover, certain of these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

Claims 4, 19, and 30 depend from claims 1, 16, and 27, respectively, and further require that generating the message further comprises generating a random component to include within the message, and that determining whether the second computer system is authorized to access the software further comprises determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message.

The Examiner cited col. 7, lines 33-55 as disclosing the requirements of claims 4, 19, and 30. (Final Office Action, pg. 3) Applicants traverse.

The cited col. 7 discusses the above discussed enablement process where the installer transmits the product name, serial number, and number of connections to a fulfillment agent, which uses this information to obtain an enabler key to return to the installer. The enabler key is then used by the enablement process to activate the license.

Nowhere does the cited col. 7 anywhere disclose the claim requirement that a random component is included in the encrypted message sent to the second computer system on which the software is installed, and that the system granting access determine whether a response from the second computer on which the software is to be installed includes the random component. Instead, the cited col. 7 mentions that the installer sends product name, serial number and number of connections information to the fulfillment agent to gain the enabler key to activate the license. Nowhere does the cited col. 7 anywhere disclose that the installer or system on which the license is to be activated send a random component that is used to determine whether the installer or enablement process may have the enabler key to activate the software.

Accordingly, amended claims 4, 19, and 30 provide additional grounds of patentability over the cited art.

Claims 7, 20, and 33 depend from claims 1, 16, and 27 and further require that the software comprises a computer program and automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system. The Examiner cited col. 7, lines 33-55 as disclosing the requirements of claims 4, 19, and 30. (Final Office Action, pg. 3) Applicants traverse.

The cited col. 7 discusses the above discussed enablement process where the installer transmits the product name, serial number, and number of connections to a fulfillment agent, which uses this information to obtain an enabler key to return to the installer. The enabler key is then used by the enablement process to activate the license.

Nowhere does the cited col. 7 anywhere disclose the claim requirement that the computer software is installed on the second computer system when the software is transmitted. Instead, the cited col. 7 teaches away from this requirement because according to the cited Ross the software is provided on a package with the computer, and then later the license must be activated by the installer on the computer in which the software is to be installed by obtaining the enabler key to decrypt the encrypted part of the license. (Ross, col. 7, lines 23-55) Thus, the cited col. 7 does not disclose, and in fact teaches away from, the claim requirement of automatically installing the software on the computer when the software is transmitted. Instead, the cited col. 7 discusses how the already provided software is activated by obtaining an enabler key that activates the license.

Accordingly, amended claims 7, 20, and 33 provide additional grounds of patentability over the cited art.

Claims 8, 21, and 34 depend from claims 1, 16, and 27, respectively, and further require that processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message. The Examiner cited col. 7, lines 33-55 as disclosing the additional requirements of these claims. (Office Action, pg. 3) Applicants traverse.

The cited col. 7 discusses the above discussed enablement process where the installer transmits the product name, serial number, and number of connections to a fulfillment agent, which uses this information to obtain an enabler key to the installer, which is used by the enablement process to activate the license.

Nowhere does the cited col. 7 anywhere disclose the claim requirement of determining whether the second computer can access the resource by determining whether the a message in the encrypted response matches a message the first computer sent to the second computer. The cited col. 7 mentions that the fulfillment agent uses information, such as product name, serial

number and connections to access an enabler key to send to the installer to activate the license. However, this cited col. 7 nowhere discloses that the fulfillment agent determine whether a message in an encrypted response from the installer matches a message the fulfillment agent sent to the installer or computer on which the program will be installed.

Accordingly, claims 8, 21, and 34 provide additional grounds of patentability over the cited art.

Amended claims 9, 11, 14, 22, 24, 26, 35, 37, and 39 depend from base claims 1, 16, and 27, and additionally require that the message transmitted to the second computer system is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system and that the encrypted response from the second computer system is encrypted with the second computer system's private key, wherein the first computer system has a public key of the second computer system for decrypting the encrypted response. The Examiner cited col. 7, lines 33-55 of Ross as disclosing the additional requirements of these claims. (Final Office Action, pg. 3) Applicants traverse for the following reasons.

The cited col. 7 discusses the above discussed enablement process where the installer transmits the product name, serial number, and number of connections to a fulfillment agent, which uses this information to obtain an enabler key to return to the installer. The enabler key is then used by the enablement process to activate the license.

These claims further require that the code made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

The Examiner cited the above discussed col. 7 as disclosing the additional requirements of these claims. (Office Action, pg. 3). For the reasons discussed above, the cited col. 7 nowhere disclose the claim requirement of determining whether there is a code made available by the second computer system, which in Ross corresponds to the installer or enabling process, that is capable of decrypting the received encrypted response, nor do these cited sections disclose that the code made available by the second computer system, i.e., the system on which the software is to be installed, comprises a public key associated with the second computer system as claimed.

Accordingly, claims 9, 11, 14, 22, 24, 26, 35, 37, and 39 provide additional grounds of patentability over the cited art.

Claims 10, 15, 23, 36, and 40 depend from claims 1, 12, 16, 27, and 38 and further require that the generated message includes a random component and a request for configuration data from the second computer system. Claims 10, 23, and 36 further require that processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software. Claims 15 and 40 further require that adding configuration data for the second computer system to the decrypted message before encrypting the message with the second computer system's private key.

The Examiner cited col. 7, lines 33-36 as disclosing the additional requirements of these claims. (Final Office Action, pg. 3) Applicants traverse for the following reasons.

The cited col. 7 mentions that an enablement process executing on the system on which the license is to be installed prompts an installer to select a product type and version. However, the claims require that the message from the first computer system that grants permission to the second computer system to access the software includes a request for configuration resources, where this message is generated in response to a request from the second computer system for the software. Nowhere does the cited col. 7 anywhere disclose that any message sent from the computer system which provides access to the software, which in the cited Ross appears to be the fulfillment agent, includes a request for configuration resources. Instead, the cited col. 7 mentions that an enablement process executing on the system on which the license is to be installed prompts an installer to select product type and version.

Accordingly, claims 10, 15, 23, 36, and 40 provide additional grounds of patentability over the cited art.

The Examiner rejected claims 5, 6, 31, and 32 as obvious (35 U.S.C. §103) over Ross in view of Komura. Applicants traverse because these claims depend from independent claims 1, 12, 16, 27, and 38, which are patentable over the cited art for the reasons discussed herein. Further, these claims provide additional grounds of distinction over the cited art for the following reasons.

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited Komura as teaching the time stamp claim requirement. (Final Office Action, pgs. 3-4) Applicants traverse.

Although the cited Komura does discuss a timestamp, nowhere does the cited Ross or Komura, alone or in combination, anywhere teach or suggest that a message generated and encrypted and sent to a second computer system, which is then included in an encrypted response by the second computer system to the first computer system, comprises a timestamp.

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons discussed above, and because they. provide further requirements on the timestamp, which is not disclosed in the cited art.

The Examiner rejected claims 2, 13, 17, and 28 as obvious (35 U.S.C. §103) over Ross in view of Jia (U.S. Patent No. 5,991,402). Applicants submit that these claims are patentable over the cited art because they depend from one of claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-40 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: January 26, 2004

By: _____
David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes Victor & Mann, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984